Vorlesung Kryptographie

WiSe '23/'24, hhu
K. Halupczok

K3: Grundlegendes zu Gruppen

Stichworte: $\mathrm{ord}(G)$, UG, Satz von Lagrange, $k \cdot a$ in $(G,+)$ und a^k in $(G,\cdot)$, $\langle a\rangle = \{k\cdot a;\ k\in\mathbb{Z}\}$ in $(G,+)$, $\langle a\rangle = \{a^k;\ k\in\mathbb{Z}\}$ in $(G,\cdot)$, $\mathrm{ord}(a) = \#\langle a\rangle$, $a^{\mathrm{ord}(G)} = 1$ in $(G,\cdot)$ ⇝ Euler-Fermat/Kleiner Fermat, schnelles Potenzieren, Lösen quadratischer Kongruenzen, Anwendung: faires Münzwurf-Knobeln am Telefon, "perfekte Faro"-Mischung von Kartenstapeln, Primitivwurzeln

---

3.1. **Einleitung:** Wir wiederholen das algebraische Konzept einer endlichen abelschen Gruppe und die wichtigsten arithmetischen/algebraischen Eigenschaften. Das schnelle Potenzieren (bei einer multiplikativ geschriebenen Gruppe) bzw. das schnelle Vervielfachen (bei einer additiv geschriebenen Gruppe) zeigt, dass hohe Potenzen auf dem Rechner schnell berechnet werden können. Die Frage, ob ein Element einer Gruppe darin ein Quadrat ist oder nicht, führt bereits zu einfachen Anwendungen, z.B. das "Münzwurf-Knobeln am Telefon". Eine Anwendung des Kleinen Fermats ist z.B. die Frage nach der Wiederholung der Kartenreihenfolge bei der "perfekten" Faro-Mischung von Karten.

Gruppen

Die Gruppen $(\mathbb{Z}_m, +, 0)$ und $(\mathbb{Z}_m^\times, \cdot, 1)$ sind **endliche** abelsche Gruppen, vgl. Def. 2.3–2.5. Da endliche Strukturen ohne "Rundungsverluste" fehlerfrei auf den Rechner übertragbar sind, sind diese für kryptographische Zwecke nützlich.

3.2. **Def.:** Die **Ordnung** einer endlichen Gruppe G ist die Anzahl ihrer Elemente, Kurz: $\mathrm{ord}(G) := \#G$.

3.3. **Def.:** Eine Teilmenge H einer Gruppe G mit Verknüpfung $*$ heißt **Untergruppe**, falls auch $(H,*)$ eine Gruppe ist. Kurz: UG. und "$H \le G$"

3.4. **Satz von Lagrange:** Ist $(G,*)$ eine endliche Gruppe, so ist die Ordnung einer Untergruppe H stets ein Teiler von $\operatorname{ord}(G)$,
Kurz: $\operatorname{ord}(H) \mid \operatorname{ord}(G)$.

Bew.: Die Linksnebenklassen $a*H := \{a*h;\ h\in H\}$ für $a\in G$ sind paarweise disjunkt, d.h. stets gilt $a*H = b*H$ oder $a*H \cap b*H = \emptyset$.
⌜Denn: Für $c\in a*H \cap b*H$ ist $c = a*g = b*h$ für $g,h\in H$, also $a = b*(h*g^{-1})$, somit $a*H = \{a*m;\ m\in H\} = \{b*h*g^{-1}*m;\ m\in H\} = \{b*m;\ m\in H\} = b*H$.⌟
Also ist G die disjunkte Vereinigung endlich vieler Linksnebenklassen $a_1*H,\dots,a_r*H$.
Da $\#(a*H) = \#H$ für alle $a\in G$ gilt, folgt mit $\operatorname{ord}(G) = r\cdot\operatorname{ord}(H)$ die Beh. □

3.5. **Def.:** Sei $(G,+)$ eine abelsche Gruppe und $a\in G$. Für $k\in\mathbb{Z}$ definieren wir $ka := a+\dots+a$ (k mal), falls $k>0$, $k\cdot 0 := 0$ und $k\cdot a := -(-k)a$ falls $k<0$.
Dann ist $\langle a\rangle := \{ka;\ k\in\mathbb{Z}\}$ eine UG von G. ⌜Klar!⌟
Wir nennen $\langle a\rangle$ die von a erzeugte UG bzw. Erzeugnis von a und a einen Erzeuger. Ist $\langle a\rangle$ endliche UG, heißt ihre Ordnung die Ordnung von a, Kurz: $\operatorname{ord}(a) := \#\langle a\rangle$.
Eine Gruppe G mit Erzeuger (z.B. Erzeuger a, so dass $G = \langle a\rangle$) heißt zyklisch. (Der Erzeuger ist i.a. nicht eindeutig bestimmt.)

3.6. Schreibt man die Gruppe multiplikativ mit Verknüpfung "$\cdot$" ("mal"), d.h. ist $(G,\cdot)$ eine Gruppe und $k\in\mathbb{Z}$, so setzt man $a^k := \underbrace{a\cdots a}_{k\text{-mal}}$ falls $k>0$, $a^0 := 1$, $a^k := (a^{(-k)})^{-1}$ falls $k<0$, und $\langle a\rangle := \{a^k;\ k\in\mathbb{Z}\}$. Ansonsten ist bis auf Schreibweise die Begrifflichkeit und Theorie zu "Erzeugern" und "Ordnungen" dieselbe.

3.7. Nach dem Satz von Lagrange gilt für jede endl. Gruppe G und $a\in G$ stets $\operatorname{ord}(a) \mid \operatorname{ord}(G)$.

3.8. **Bsp.:** $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z} = \{0, 1, \dots, m-1\}$ ist "die" zyklische Gruppe G mit $\text{ord}(G) = m$.
Ist $m = p$ prim, können außer $\{0\}$ und $\mathbb{Z}/p\mathbb{Z}$ keine weiteren UG ex.

3.9. **Lemma:** Sei $(G, +)$ Gruppe, $a \in G$. Es ist $\text{ord}(a)$ die kleinste natürliche Zahl m mit $ma = 0$. Es gilt: $ka = 0 \iff \text{ord}(a) \mid k$.
(Bei multiplikativer Schreibweise: $\text{ord}(a) = \min\{m \in \mathbb{N} : a^m = 1\}$ und $a^k = 1 \iff \text{ord}(a) \mid k$.)
Bew.: Erster Teil klar, zweiter Teil: "$\Rightarrow$": Falls $k \in \mathbb{N}$ mit $ka = 0$ ist, nehme Division von k durch $\text{ord}(a)$ vor: $k = q \cdot \text{ord}(a) + r$ mit $0 \le r < \text{ord}(a)$. Wegen $0 = ka = q \cdot \underbrace{\text{ord}(a) \cdot a}_{=0} + ra$ folgt $ra = 0$, wegen der Minimalität von $\text{ord}(a)$ also $r = 0$, also $\text{ord}(a) \mid k$.
"$\Leftarrow$": Für $k = m \cdot \text{ord}(a)$ folgt $ka = m \cdot (\underbrace{\text{ord}(a) \cdot a}_{=0}) = 0$. □

3.10. **Folgerung:** $\text{ord}(G) \cdot a = 0$ bzw. multiplikativ: $a^{\text{ord}(G)} = 1$ [da $\text{ord}(a) \mid \text{ord}(G)$ nach Lemma 3.9.]

3.11. **Folgerung:** Da $\text{ord}((\mathbb{Z}/m\mathbb{Z})^\times) = \varphi(m)$, ist $a^{\varphi(m)} \equiv 1 \bmod m$, falls $\text{ggT}(a, m) = 1$.
Für p prim: $a^{p-1} \equiv 1 \bmod p$ für $p \nmid a$.
(Korollar aus 3.10.) "Kleiner Satz von Fermat"

3.12. **Bem.:** Die Kongruenz $a^{\varphi(m)} \equiv 1 \bmod m$, falls $\text{ggT}(a, m) = 1$, heißt auch "Satz von Euler-Fermat". Als Ordnung eines $a \in \mathbb{Z}_m^\times$ (Notation: $\text{ord}_m(a)$) kommt also nur ein Teiler von $\varphi(m)$ in Frage.

3.13. **Bsp.:** Haben $\varphi(15) = \varphi(3 \cdot 5) = \varphi(3) \cdot \varphi(5) = 2 \cdot 4 = 8$. Die möglichen Ordnungen von Zahlen $a \bmod 15$, wo $\text{ggT}(a, 15) = 1$ ist, sind also $1, 2, 4, 8$.
Wegen $4^2 = 16 \equiv 1 \ (15)$ ist z.B. $\text{ord}_{15}(4) = 2$. Bei größeren Zahlen muss man u.U. Potenzen mit größeren Exponenten ausrechnen, um die Ordnung zu bestimmen.

3.14. Generell stellt sich in Anwendungen die Frage, wie man leicht und schnell (modulare) Potenzen $a^k \bmod m$ mit großem k berechnen kann.
Der Satz von Euler-Fermat erlaubt bereits eine Reduktion von $k \bmod \varphi(m)$:
Ist $k = q \cdot \varphi(m) + r$ mit $0 \le r < \varphi(m)$, folgt $a^q = a^{\varphi(m)\cdot q + r} = (a^{\varphi(m)})^q \cdot a^r$
$\equiv 1^q \cdot a^r = a^r \bmod m$. Ist aber auch $\varphi(m)$ bzw. r groß*, hilft man sich mit folgender

* oder $\varphi(m)$ nicht berechenbar

3.15. Methode des schnellen Potenzierens / "square-and-multiply"-Verfahrens weiter:
Geg. sei eine Gruppe $(G, \cdot)$, zu berechnen ist für $r \in \mathbb{N}$, $a \in G$
die Potenz $a^r := \underbrace{a \cdots a}_{r\text{-mal}}$ in der Gruppe G.

1. Schritt: Mit höchstens $d := \lfloor \frac{\log(r)}{\log(2)} \rfloor$ vielen Verknüpfungen in G berechne durch sukzessives Quadrieren: $a^2 = a \circ a$, $a^{2^2} = a^4 = (a^2) \circ (a^2)$, $a^{2^3} = (a^{2^2}) \circ (a^{2^2})$, $a^{2^4} = (a^{2^3}) \circ (a^{2^3})$, $\dots$, a^{2^d}

2. Schritt: Schreiben r als Binärzahl: $r = \sum_{i=0}^{d} c_i 2^i$ mit $c_i \in \{0,1\}$.

3. Schritt: Berechnen $a^r = a^{c_0} \cdot a^{2c_1} \cdot a^{2^2 c_2} \cdots a^{2^d c_d} = (a^{c_0}) \circ (a^2)^{c_1} \circ (a^{2^2})^{c_2} \circ \cdots \circ (a^{2^d})^{c_d}$
mit maximal d weiteren Verknüpfungen in G.

Somit reichen höchstens $2d = O(\log(r))$ viele Anwendungen der Gruppenverknüpfung "$\circ$".
Das ist deutlich schneller als das naive Ausrechnen mit $r-1 = O(r)$ vielen Verknüpfungen.

3.16. Bei additiver Schreibweise einer Gruppe $(G, +)$ geht das Verfahren zur Berechnung von $r \cdot a$ analog. Man nennt es dann auch das "dual-and-add"-Verfahren / schnelles Vervielfachen.
Dann anstelle Quadrierungen nimmt man Verdopplungen, und die Verknüpfungen sind dann das Anwenden der Gruppenaddition "+" in G.

3.17. Bsp.: $5^{12} = 5^{2^2+2^3} = 5^{2^2} \cdot 5^{2^3}$, modulo 11 rechnen wir: $5^2 \equiv 3 \,(11)$, $5^{2^2} \equiv 3^2 \equiv -2 \,(11)$, $5^{2^3} \equiv (-2)^2 \equiv 4 \,(11)$,
also $5^{12} \equiv (-2) \cdot 4 \equiv 3 \,(11)$; geht schneller als $5^{12} = 244140625$ von Hand durch 11 zu teilen
bzw. das 9 auszurechnen... (∇ $5^{2^3} = 5^{(2^3)} = 5^8 \neq (5^2)^3 = 5^{2\cdot 3} = 5^6$)

Bsp.: Endziffer von 127^{12}? Mod 10 berechne $127^{12} \equiv 7^{12} \equiv 7^2 \cdot 7^2 \cdot 7^2 \equiv 1 \cdot 1 = 1 \,(10)$, da $7^2 \equiv 9$, $7^{2^2} \equiv 9^2 \equiv 1$, $7^{2^3} \equiv 1^2 \equiv 1$.

3.18. **Eine Anwendung des Kleinen Fermats**

Im Fall $p \equiv 3\ (4)$ prim können wir Lösungen quadratischer Kongruenzen mod p bestimmen: Sei $p = 4k+3$ prim und a mit $p \nmid a$ ein quadratischer Rest mod p, d.h. es ex. ein $b \in \mathbb{Z}$ mit $a \equiv b^2\ (p)$, und wir möchten $\pm b$ mod p ausrechnen können. Nach dem Kleinen Fermat folgt $b^{4k+2} = b^{p-1} \equiv 1\ (p)$.

Es folgt: $(a^{k+1})^2 \equiv (b^2)^{2(k+1)} = b^{(4k+2)+2} \equiv 1 \cdot b^2 \equiv a\ (p)$,
d.h. die Lösungen von $b^2 \equiv a\ (p)$ sind $b = \pm a^{k+1}\ (p)$. $\equiv \pm a^{\frac{p+1}{4}}\ (p)$
Da $a^{k+1} \not\equiv -a^{k+1}\ (p) \Leftrightarrow 2a^{k+1} \not\equiv 0\ (p)$, gibt es genau 2 Lösungen mod p, die wir etwa im Restsystem $\{0, 1, \dots, p-1\}$ angeben können und mit $\pm a^{k+1}$ mod p berechnen können, z.B. mit dem schnellen Potenzieren.

3.19. **Bsp.:** Für $p = 47 \equiv 3\ (4)$ betr. $a = 17$. Haben $47 = 4 \cdot 11 + 3$, also $k = 11$.
Die Kongruenz $a \equiv b^2\ (p)$ hat die Lösungen $\pm a^{k+1} \equiv \pm 17^{12}\ (47)$.
Mit $12 = 1 \cdot 2^3 + 1 \cdot 2^2$ berechnen wir die Potenz mit schnellem Potenzieren:

- $17^2 = 289 \equiv 7\ (47) \overset{(\cdot)^2}{\rightsquigarrow} 17^{2^2} \equiv 7 \cdot 7 = 49 \equiv 2\ (47) \overset{(\cdot)^2}{\rightsquigarrow} 17^{2^3} \equiv 2 \cdot 2 = 4\ (47)$
- $17^{12} = 17^{2^3 + 2^2} = 17^{2^3} \cdot 17^{2^2} \equiv 4 \cdot 2 = 8\ (47)$

Probe: $(\pm 8)^2 = 64 \equiv 17\ (47)$ ✓

3.20. Sei nun n eine zus.gesetzte Zahl, etwa $n = p \cdot q$ mit $p \equiv q \equiv 3\ (4)$ prim, etwa $p = 4k+3$, $q = 4l+3$ mit $k, l \in \mathbb{N}_0$, und sei $p \neq q$. (p, q bekannt)
Sei a mod n ein quadratischer Rest mod n, d.h. es existiere ein $b \in \mathbb{Z}$ mit $a \equiv b^2\ (n)$.
Gesucht seien die Lösungen der Kongruenz $a \equiv x^2\ (n)$.
Nach dem CRS gilt: $x^2 \equiv a\ (n) \Leftrightarrow x^2 \equiv a\ (p)$ und $x^2 \equiv a\ (q)$, und die jeweiligen Lösungen $\pm a^{k+1}$ mod p und $\pm a^{l+1}$ mod q kann man zusammensetzen zu (maximal) vier Lösungen mod n.

3.21. Es sind genau 4 Lösungen, die explizit wie folgt bestimmt werden können:

Sind $r, s \in \mathbb{Z}$ geg. mit $rp + sq = 1$, d.h. die Bézout-Elemente von p und q, und ist $\pm b$ Lsg. von $x^2 \equiv a \ (p)$ [2 Mögl.]
$\pm c$ Lsg. von $x^2 \equiv a \ (q)$ [2 Mögl.],
so liefert die CRS-Formel (Inv. von q mod p, Inv. von p mod q)

$$x = \pm b\, s\, q \pm c\, r\, p$$

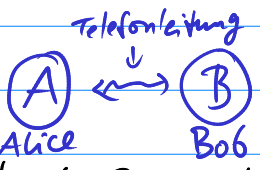
genau vier Lösungen von $x^2 \equiv a \ (p \cdot q)$. Diese müssen paarweise inkongruent mod pq sein, da wir laut CRS den Ringiso $\mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q$ haben und die 4 versch. Lösungspaare $(b, c), (-b, c), (b, -c), (-b, -c)$ auf der r.S. des Isos, denen genau 4 Restklassen in $\mathbb{Z}_{pq}$ auf der l.S. des Isos entsprechen.

alternativ: $r \equiv p^{q-2} \ (q)$, da $p \cdot p^{q-2} \equiv p^{q-1} \equiv 1 \ (q)$, analog $s \equiv q^{p-2} \ (p)$.

3.22. Bsp.: Betr. $p = 11$, $q = 19$, d.h. $k = 2$, $\ell = 4$. Wähle $a = 47$. ($3 = k+1$)
Die Lösungen von $x^2 \equiv 47 \equiv 3 \ (11)$ sind $\pm 3^3 \ (11) \equiv \pm 5 \ (11)$,
die Lösungen von $x^2 \equiv 47 \equiv 9 \ (19)$ sind $\pm 3 \ (19)$.
Bézout-E!. bestimmen (hier Probieren): Inv. von $19 \equiv 8 \bmod 11$ ist 7, Inv. von $11 \bmod 19$ ist 7.
$\rightsquigarrow s = r = 7$ und $x \equiv \mp 5 \cdot 7 \cdot 19 \mp 3 \cdot 7 \cdot 11 \ (11 \cdot 19)$ laut CRS
ergibt $x \in \{\pm 16, \pm 60\}$. Probe: $16^2 \equiv 47 \ (11 \cdot 19)$ ✓, $60^2 \equiv 47 \ (11 \cdot 19)$ ✓

Man beachte, dass wir hier benötigen, dass a ein quadratischer Rest mod 11 und mod 19 sein muss. Würde man a zufällig wählen, wäre das nicht unbedingt der Fall; dann ist $x^2 \equiv a \ (n)$ ohnehin unlösbar, falls a kein quadratischer Rest mod $11 \cdot 19$ ist. Mit der Formel a^{k+1} mod 11 bzw. 19 würde man keine modulare Quadratwurzel erhalten: Bsp.: $p = 47$, $a = 5$: Mit $a^{k+1} = 5^{12} \equiv 18 \ (47)$
ist $(\pm 18)^2 \equiv 42 \equiv -5 \not\equiv 5 \ (47)$.

Eine Anwendung:



3.23. Problem des fairen Münzwurfknobelns am Telefon:

Zwei Spieler, Alice (A) und Bob (B) möchten etwas ausknobeln (z.B. wer beim Fernschach beginnen soll und dann einen Vorteil hat, etc.), allerdings sprechen sie sich am Telefon oder mailen sich, und können sich daher nicht sehen. (A) wirft eine Münze, und (B) denkt vorher "Kopf" oder "Zahl", verrät das aber nicht. (Wäre (B) life dabei, würde er "Kopf" oder "Zahl" sagen und das Ergebnis sehen. Am Telefon gilt: Würde (A) seine Wahl vorher kennen, so würde (B) ihr mitgeteiltes Münzwurfergebnis u.U. anzweifeln.)

(A) teilt (B) das Ergebnis mit, und (B) verkündet, wer gewonnen hat: (A), wenn ihr Münzwurfergebnis mit der Wahl von (B) übereinstimmt, ansonsten gewinnt (B). Sei (B)s geheime Wahl "Zahl".

Teilt (A) mit, dass sie "Zahl" geworfen hat, akzeptieren (A) und (B) den Spielausgang, weil dann (A) gewinnt und (B) ihr das verkündet. Falls (A) jedoch mitteilt, dass sie "Kopf" geworfen hat, teilt (B) mit, dass (A) verloren habe, was (A) natürlich nicht akzeptieren würde.

↝ Problem: Wie kann bei Ergebnis "Kopf" Spieler (B) ihre Mitspielerin (A) überzeugen, dass er vor dem Münzwurf die Wahl "Zahl" getroffen hat?

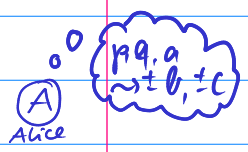
Unsere Antwort: Wenn (B) dann ein "Geheimnis" von (A) nennt, das nur sie (und (B)) wissen kann, und nie über den öffentlich zugänglichen Kommunikationskanal ausgetauscht wurde. Das ist z.B. der Fall, wenn (B) dann eine Zahl $n = pq$ faktorisieren könnte, deren Primteiler p, q ansonsten nur (A) kennt!

3.24. Das Verfahren funktioniert wie folgt:

Schritt (1.) Ⓐ wählt Primzahlen $p, q \equiv 3 (4)$, $p \neq q$, berechnet $n = p \cdot q$ und schickt n an Ⓑ

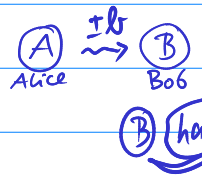
Schritt (2.) Ⓑ wählt $1 < b < n-1$ zufällig und behält b geheim, er berechnet $a \equiv b^2 (n)$, und schickt a an Ⓐ

Schritt (3.) Ⓐ berechnet die 4 Lösungen von $x^2 \equiv a (n)$ mit der Berechnungsmethode aus 320/21, die 4 Lösungen seien $\pm b, \pm c \in \mathbb{Z}$, (mit b von Ⓑ), die Lösungen $\pm c$ sind andere, die Ⓑ nicht kennt. Soweit die Vorbereitung; dann der eigentliche Münzwurf:



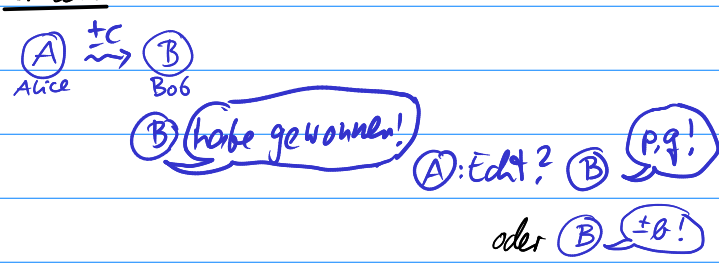
Schritt (4.) Ⓐ wählt eine der 4 Lösungen zufällig aus (etwa durch Münzwurf!), d.h. entweder $\pm b$ oder $\pm c$, und schickt Ⓑ das Ergebnis.
Ⓐ kann nicht wissen, dass Ⓑ die Zahl b gewählt hat. Die Vereinbarung ist nun: Schickt Ⓐ eine der Zahlen $\pm b$, gewinnt Ⓐ,
schickt Ⓐ eine der Zahlen $\pm c$, gewinnt Ⓑ, und das verkündet Ⓑ.

1. Fall:



ODER

2. Fall:



Schritt (5.) Es erfolgt die Verifikation, dass Ⓐ wirklich verloren hat im 2. Fall, dann muss sich Ⓐ davon überzeugen, dass Ⓑ vorher wirklich $\pm b$ gewählt hat:
✓ Es kann Ⓐ die Lösungen $\pm b$ einfach mitteilen, da Ⓐ auch diese berechnet hat.
✓ Alternativ kann Ⓑ ihr sogar die Primfaktoren von n nennen:

(B) berechnet $b+c \bmod n$ und

$d = ggT(b+c, n)$ mit dem euklidischen Algo.

Dann ist $d=p$ oder $d=q$. [Denn aus $b^2 \equiv a \equiv c^2 \ (pq)$ folgt:
$pq \mid (b-c)(b+c) = b^2 - c^2$, und da $b \not\equiv c \ (p)$, $b \not\equiv c \ (q)$ folgt $q \mid b+c$ oder $p \mid b+c$,
und $d \neq n$, weil sonst $b \equiv -c \bmod n$ wäre ↯.]

Also kann (B), weil er c kennt, die von (A) gewählten Primfaktoren bestimmen und (A) mitteilen und auf diese Art (A) überzeugen.

Das konnte (B) nur, weil er vorher auch wirklich die nicht von (A) genannte Lösung $\pm b$ hatte. Damit ist das Spiel fair.

3.25. Bem.: • Für die Praxis wird dies unsetzbar sein, wenn man leicht große Primzahlen $\equiv 3 \ (4)$ erzeugen kann. Dieses Problem der Primzahlerzeugung wird in K7/K8 behandelt werden.

• Ein zu 3.24 verwandtes Verfahren ist der Fiat-Shamir-Algorithmus, der ebenso darauf beruht, dass Quadratwurzelziehen mod $n=pq$ schwer ist, vgl. [Bentelspacher et al., Kap. 4.2].

3.26. Bem.: Das Verfahren beruht speziell auf der Isomorphie $\mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q$ laut CRS. Damit konnte der Ring $\mathbb{Z}_{pq}$ in ein Produkt von zwei Teilringen "zerlegt" werden. Für die PFZ $n = p_1^{e_1} \cdots p_r^{e_r}$ erhalten wir laut CRS den Ringiso $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_r^{e_r}}$.

3.27. Wir erinnern an den Hauptsatz über endlich erzeugte R-Moduln (R=HIB) aus der Algebra, nach dem jede endl. erz. R-Modul in ein Produkt von zyklischen unzerlegbaren R-Moduln zerlegt werden kann (Algebra A 17.12).

Da $\mathbb{Z}$-Moduln gerade abelsche Gruppen sind, beinhaltet dies auch den Hauptsatz über endlich erzeugte abelsche Gruppen (Algebra A 7.15),

nachdem gilt: A endl. erz. ab. Gr. $\Rightarrow A \cong \mathbb{Z}^m \oplus \bigoplus_{p \in P} \bigoplus_{i=1}^{n_p} \mathbb{Z}_{p^{e_i(p)}}$.

Beachten Sie, dass eine zyklische Gruppe $\mathbb{Z}_{p^e}$ nicht weiter zerlegt werden kann.

[Wäre etwa $\mathbb{Z}_{p^e} \cong \mathbb{Z}_{p^{e_1}} \times \mathbb{Z}_{p^{e_2}}$ mit $e_1 + e_2 = e$, wo $e_1 \leq e_2 < e$, hätte jedes El. der r.S. eine Ordnung $\leq p^{e_2} = kgV(p^{e_1}, p^{e_2})$, auf der l.S. ex. aber Erzeuger mit Ordnung $p^e > p^{e_2}$.]

3.28. Eine (andere) Anwendung des Kleinen Satzes von Fermat 3.11 ist das "perfekte" Kartenmischen (engl. perfect faro shuffle); diese ist keine Zufallsmischung: Bei diesem wird ein Kartenstapel aus 52 Karten in zwei Teile von je 26 Karten geteilt und diese jeweils abwechselnd in einen neuen Stapel eingefügt: Die Karten Nr. 1, 2, ..., 26 geraten im neuen Stapel an Position 2, 4, 6, ..., 52, und die Karten Nr. 27, 28, ..., 52 geraten im neuen Stapel an Position 1, 3, 5, ..., 51.
Ist x die Nr. der ursprünglichen Karte, so ist die neue Position y also $1 \le y \le 52$ mit $2x \equiv y \ (53)$. [$2 \cdot 27 = 54 \equiv 1 \ (53)$, $2 \cdot 28 = 56 \equiv 3 \ (53)$, ...]

Nach n vielen solcher Mischungen/Shuffles gerät jede Karte x an die Position $2^n x \ (53)$.

3.29. Frage: Wann ist diese wieder x für jede Karte x, d.h. wann gelangt der Stapel wieder in die Ausgangsreihenfolge zurück?
Offenbar dann, wenn $2^n x \equiv x \ (53)$ für alle x, d.h. $2^n \equiv 1 \ (53)$.
Da wir wissen, dass 53 prim ist, gilt $2^{52} \equiv 1 \ (53)$ laut Kleinem Fermat, d.h. nach 52 Shuffles kehrt der Stapel wieder in die Ausgangsreihenfolge zurück.
Es gilt $\mathrm{ord}_{53}(2) = 52$, d.h. 2 ist eine Primitivwurzel mod 53 [$2^{13} \equiv 30 \not\equiv 1 \ (53)$, $2^2, 2^4, 2^{26} \equiv -1$] deswegen klappt dies nicht früher als nach 52 Shuffles.

3.30. Bem.: Bei 62 Karten bräuchte es nur 6 Shuffles, da $2^6 - 1 = 63$.
Bei $p-1$ Karten (p prim) werden $p-1$ Shuffles benötigt, wenn 2 eine PW mod p ist.
Laut Artinscher PW-Vermutung (vgl. K7) ist dies für vermutlich unendlich viele Pzen p so. Erinnerung an Einh.T, EZG, über Primitivwurzeln:

3.31. Def.: Für $m \in \mathbb{N}$ heißt ein $a \in \mathbb{Z}$ mit $(a,m)=1$ eine Primitivwurzel modulo m (Kurz: PW mod m), falls $\mathrm{ord}_m(a) = \varphi(m)$ ist, d.h. wenn a Erzeuger von $\mathbb{Z}_m^\times$ ist. } Eine PW ist ein El. von $\mathbb{Z}_m^\times$ mit maximalmöglicher Ordnung $\varphi(m)$

3.32. Satz von Euler über Primitivwurzeln: Zu $m \in \mathbb{N}$ existiert genau dann eine PW mod m, wenn $m \in \{1,2,4\} \cup \{p^k; p>2 \text{ prim}, k \in \mathbb{N}\} \cup \{2p^k; p>2 \text{ prim}, k \in \mathbb{N}\}$ ist.